

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION

---

UNITED STATES OF AMERICA	§	
	§	
v.	§	Case No: 3:12-CR-413-L
	§	Hon. Sam A. Lindsay
BARRETT LANCASTER BROWN	§	

**MOTION TO DISMISS THE INDICTMENT**

Defendant BARRETT LANCASTER BROWN files this motion to dismiss Count 1 and Counts 3–12 of the Indictment. In support thereof, he would show the Court the following:

**Table of Contents**

Table of Contents.....	i
Table of Cases.....	iii
Introduction.....	1
Statement of Facts.....	2
A. Barrett Brown.....	1
B. Project PM.....	2
C. The Hack of Stratfor Forecasting, Inc.....	3
D. Publication of Stratfor Files Occurred Before and After Dec. 25, 2011.....	4
E. Conduct Giving Rise to the Indictment.....	7
Argument .....	9
I. THE COURT SHOULD DISMISS COUNT 1 & COUNTS 3–12 FOR FAILURE TO ALLEGE AN OFFENSE.....	8
A. The Legal Standard for Dismissal.....	8
B. The Charging Statutes.....	8
i. Count 1 Charges a Violation of 18 U.S.C. §1028(a)(2).....	8
ii. Counts 3–12 Charge Violations of 18 U.S.C. §1028A(a)(1).....	9
iii. Count 1 is a Predicate to Counts 3–12.....	9
C. The Statutory Terms at Issue.....	10

i. The Meaning of “Authentication Feature” Under §1028 .....	10
ii. The Meaning of “Transfer” Under §1028.....	11
D. Count 1 Fails to Allege “Authentication Features” Within the Meaning of §1028.....	12
E. Count 1 Fails to Allege a “Transfer” of CVVs.....	15
i. The Hyperlink that Mr. Brown is Alleged to Have Republished did not Contain CVVs.....	15
ii. By Republishing a Hyperlink, Mr. Brown Did Not Make the Stratfor File “Available To Other Persons Online” .....	16
F. A Dismissal of Count 1 (and Counts 3–12) Would Be in Line With This Court’s Ruling in <i>Live Nation Motor Sports, Inc.</i> .....	18
G. Constitutional Avoidance Warrants Dismissal of Count 1 (& Counts 3–12).....	20
 II. THE COURT SHOULD DISMISS COUNT 1 & COUNTS 3-12 FOR PENALIZING CONDUCT PROTECTED BY THE FIRST AMENDMENT.....	21
 A. The Application of §1028(a)(2) to Mr. Brown’s Speech Warrants Strict Scrutiny.....	21
i. Mr. Brown’s Republication of a Hyperlink is Protected Speech .....	21
ii. 1028(a)(2) Seeks to Punish Pure Political Speech and Routine Newsgathering on the Basis of its Content.....	23
iii. Mr. Brown’s Conduct is Not “Speech Integral to Criminal Conduct”.....	25
 B. Section 1028(a)(2) Cannot Survive Strict Constitutional Scrutiny.....	26
C. Applying <i>Bartnicki v. Vopper</i> to Mr. Brown’s Republication of a Hyperlink Commands a Dismissal of Count 1 and Counts 3–12.....	28
D. Section 1028(a)(2) Cannot Survive Intermediate Constitutional Scrutiny.....	29
 III. THE COURT SHOULD DISMISS COUNT 1 AND COUNTS 3–12 AS UNCONSTITUTIONALLY VAGUE AND OVERBROAD.....	31
 A. Sections 1028(a)(2) is Unconstitutionally Vague on its Face.....	31
B. As Applied to Mr. Brown Section 1028(a)(2) is Unconstitutionally Vague.....	32
C. 1028(a)(2) is Overbroad Because it Prohibits a Substantial Amount of Protected Speech.....	34

**Table of Authorities and Cases**

<i>ACTV, Inc. v. Walt Disney Co.</i> , 346 F.3d 1082 (Fed. Cir. 2003) .....	16
<i>Arista Records, Inc. v. Mp3Board, Inc.</i> , 2002 Copr. L. Dec. P 28483 (S.D. N.Y. 2002) .....	19
<i>Ashcroft v. Free Speech Coal.</i> , 535 U.S. 234 (2002).....	25, 26
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001).....	23, 26, 27, 28
<i>Bensusan Restaurant Corp. v. King</i> , 126 F.3d 25 (2nd Cir. 1997) .....	16
<i>Bernstein v. JC Penney, Inc.</i> , 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998).....	19
<i>Bouie v. City of Columbia</i> , 378 U.S. 347 (1964) .....	10
<i>Branzburg v. Hayes</i> , 408 U.S. 665 (1972) .....	24
<i>Brown v. Entertainment Merchants Ass'n</i> , — U.S. —, 131 S.Ct. 2729 (2011).....	26
<i>Buckley v. Am. Constitutional Law Found., Inc.</i> , 525 U.S. 182 (1999) .....	22
<i>Buckley v. Valeo</i> , 424 U.S. 1, 17 (1976) .....	30
<i>Cohen v. California</i> , 403 U.S. 15 (1971).....	23
<i>Cox Broadcasting Corp. v. Cohn</i> , 420 U.S. 469 (1975).....	23, 27
<i>Duke v. Univ. of Texas at El Paso</i> , 663 F.2d 522 (5th Cir. 1981).....	10
<i>Duncan v. Walker</i> , 533 U.S. 167 (2001).....	14
<i>Dunn v. United States</i> , 442 U.S. 100 (1979) .....	10
<i>First National Bank v. Bellotti</i> , 435 U.S. 765 (1978).....	24
<i>Giboney v. Empire Storage &amp; Ice, Co.</i> , 336 U.S. 490 (1949).....	25
<i>Grayned v. City of Rockford</i> , 408 U.S. 104 (1972) .....	32
<i>Hersh v. U.S. ex rel. Mukasey</i> , 553 F.3d 743 (5th Cir. 2008).....	34
<i>In re Camp</i> , 631 F.3d 757 (5th Cir. 2011).....	10

<i>Joseph Burstyn, Inc. v. Wilson</i> , 343 U.S. 495 (1952).....	22
<i>Kokoszka v. Belford</i> , 417 U.S. 642 (1974).....	14
<i>Live Nation Motor Sports, Inc. v. Davis</i> , 2006 WL 3616983 (N.D.Tx. 2006).....	18, 20
<i>Marks v. United States</i> , 430 U.S. 188 (1977).....	10
<i>McIntyre v. Ohio Elections Comm’n.</i> , 514 U.S. 334 (1995) .....	24
<i>Multimedia Holdings Corp. v. Circuit Court of Florida</i> , 544 U.S. 1301 (2005).....	35
<i>New York Times Co. v. Sullivan</i> , 376 U.S. 254 (1964) .....	22
<i>New York v. Ferber</i> , 458 U.S. 747 (1982).....	25
<i>Obsidian Fin. Grp., LLC v. Crystal Cox</i> 740 F.3d 1284 (9 <sup>th</sup> Cir. Jan. 17, 2014).....	23
<i>Online Policy Group v. Diebold, Inc.</i> , 337 F. Supp. 2d 1195 (N.D. Cal. 2004).....	19
<i>Perfect 10 v. Google, Inc.</i> , 416 F. Supp. 2d 828 (C.D. Cal. 2006) .....	15
<i>Rabe v. Washington</i> , 405 U.S. 313 (1972).....	10
<i>RAV v. City of St. Paul</i> , 505 U.S. 377 (1992).....	24, 26
<i>Reno v. American Civil Liberties Union</i> , 512 U.S. 844 (1997) .....	17
<i>Scales v. United States</i> , 367 U.S. 203 (1961).....	35
<i>Sheppard v. Maxwell</i> , 384 U.S. 333 (1966).....	22
<i>Simon &amp; Schuster, Inc. v. Members N.Y. State Crime Victims Board</i> , 502 U.S. 105 (1991).....	25
<i>Smith v. Daily Mail Pub. Co.</i> , 443 U.S. 97 (1979).....	27, 29
<i>Sutcliffe v. Epping</i> , 584 F.3d 314 (1st Cir.2009) .....	22
<i>Texas v. Johnson</i> , 491 U.S. 397 (1989).....	22
<i>The Florida Star v. B.J.F.</i> , 491 U.S. 524 (1989).....	27
<i>Thornhill v. Alabama</i> , 310 U.S. 88 (1940).....	22
<i>Ticketmaster Corp. v. Tickets.Com, Inc.</i> , 54 U.S.P.Q.2d 1344 (C.D. Cal. 2000) .....	19

<i>U.S. v. Fuller</i> , 531 F.3d 1020 (9th Cir. 2008) .....	13
<i>U.S. v. Jaensch</i> , 665 F.3d 83 (4th Cir. 2011) .....	13
<i>U.S. v. Spears</i> , 697 F.3d 592 (7th Cir. 2012) .....	12
<i>United Sav. Ass'n of Tex. v. Timbers of Inwood Forest Associates Ltd.</i> , 484 U.S. 365 (1988) .....	14
<i>United States v. Am. Soc. of Composers, Authors, Publishers</i> , 627 F.3d 64 (2d Cir. 2010) .....	20
<i>United States v. Cline</i> , 286 Fed. Appx. 817 (4th Cir. 2008) .....	13
<i>United States v. Fontenot</i> , 665 F.3d 640 (5th Cir. 2011) .....	8
<i>United States v. Hall</i> , 704 F.3d 1317 (11th Cir. 2013) .....	12
<i>United States v. National Treasury Employees Union</i> , 513 U.S. 454 (1995) .....	30
<i>United States v. O'Brien</i> , 391 U.S. 367, 88 S.Ct. 1673 (1968) .....	30
<i>United States v. Payne</i> , 341 F.3d 393 (5th Cir. 2003) .....	8
<i>United States v. Playboy Entertainment Group, Inc.</i> , 529 U.S. 803 (2000) .....	25
<i>United States v. Stock</i> , 728 F.3d 287 (3d Cir. 2013) .....	8
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2d Cir. 2001) .....	15, 22
<i>Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.</i> , 455 U.S. 489 (1982) .....	32
<i>Virginia State Bd. of Pharm. v. Virginia Citizens Consumer Council</i> , 425 U.S. 748 (1976) .....	22
<i>Virginia v. Black</i> , 538 U.S. 343 (2003) .....	24
<i>Worrell Newspapers of Ind., Inc. v. Westhafer</i> , 739 F.2d 1219 (7th Cir. 1984) .....	29

## Statutes

18 U.S.C. § 1028 (a)(1–4) .....	13
18 U.S.C. § 1028(a)(2) .....	8, 33, 34
18 U.S.C. § 1028(a)(7) .....	14, 32
18 U.S.C. § 1028(b)(1)(A–B) .....	13

18 U.S.C. § 1028(b)(2)(A).....	13
18 U.S.C. § 1028(c)(3)(A).....	9
18 U.S.C. § 1028(d)(1) .....	10, 32
18 U.S.C. § 1028(d)(10).....	12
18 U.S.C. § 1028(d)(6)(A) .....	11
18 U.S.C. § 1028(d)(7) .....	14, 32
18 U.S.C. § 1028A(c)(4).....	9
18 U.S.C.A. § 1028A(a)(1) (West).....	9
F.R.Cr.P. Rule 12(b).....	8
SAFE ID Act of 2003, Pub. L. No. 108–21, § 607, 117 Stat. 650 (2003).....	11

### **Other Authorities**

3-Digit Security Code, Visa .....	13
BLACK'S LAW DICTIONARY (9th ed. 2009).....	12, 17
Financial Glossary and Terms, Discover Card .....	13
H. Conf. Rep. No. 108–66 (2003), [2003 U.S.C.C.A.N. 683].....	11
Model Penal Code §5.01(b) (Official Draft, 1985) .....	18
Stephen A. Siegel, The Origin of the Compelling State Interest Test and Strict Scrutiny, 48 Am. J. Legal Hist. 355 (2006).....	26
<i>Transfer Definition</i> , MERRIAM-WEBSTER DICTIONARY .....	12

### **Treatises**

2 A J. Sutherland, Statutes and Statutory Construction § 47.02 (5th ed., Norman Singer ed.).....	14
--	----

3 Norman J. Singer, Sutherland Statutes and Statutory Construction § 59:3 (6th ed. 2005) .....	10
--	----

## INTRODUCTION

In Count 1 (and Counts 3–12) of the Superseding Indictment (“Indictment”), Mr. Brown is charged for republishing a hyperlink from one public chat room on the Internet to another. As detailed below, this case, and these motions present First Amendment issues of overwhelming importance.

As set forth in POINT I, the Indictment fails in many respects to state an offense under Count 1 and Counts 3–12 (for which Count 1 is a predicate). As a matter of pleading, the Indictment is fatally flawed because (1) it fails to allege an essential element altogether—“the transfer of *authentication features*,” and (2) it fails to allege that Mr. Brown transferred *anything* other than a hyperlink. Instead, the government claims that Mr. Brown violated the statute because by republishing a (publicly available) hyperlink, he caused a (publicly available) file to be “made available” to others online.” However, the government’s theory fails to satisfy any valid construction of the charging statutes.

As addressed in POINT II, the criminalization of Mr. Brown’s speech (by republishing the hyperlink) is an unconstitutional abridgement of the First Amendment because it regulates pure political speech based on its content, which compels strict scrutiny. The alleged conduct also falls squarely under a recent Supreme Court case that compels dismissal. Also Count 1 and Counts 3–12 would fail under intermediate scrutiny if put to the test.

Finally, as set forth in POINT III, if (notwithstanding the plain meaning, the legislative history, and applicable case law) somehow the alleged conduct is deemed to be encompassed by the charging statutes, then they are unconstitutionally vague on their face and as applied. Additionally, they would be unconstitutionally overbroad and chill speech in violation of the First Amendment.



## **STATEMENT OF FACTS**

### **A. Barrett Brown**

Barrett Lancaster Brown is a thirty-two year old American satirist, author and journalist. His work has appeared in Vanity Fair, the Guardian, Huffington Post, True/Slant, the Skeptical Inquirer and many other outlets. *See* Summary Chart of Select Publications by Barrett Brown, (03:CR:317, Dkt. 90 Exh. A). He is the co-author of a satirical book on creationism entitled *Flock of Dodos: Behind Modern Creationism, Intelligent Design and the Easter Bunny*. As described by Alan Dershowitz, Felix Frankfurter Professor of Law at Harvard Law School, “Flock of Dodos is in the great tradition of debunkers with a sense of humor, from Thomas Paine to Mark Twain.” *See Id.* (Exh. B). Indeed, Mr. Brown’s use of sarcasm, humor and hyperbole, used often to describe serious subject matter, has caused his admirers (and critics) to compare him to journalism icons such as Hunter S. Thompson. *See Id.* (Exh. C).

### **B. Project PM**

In 2009, Mr. Brown founded Project PM, a collaborative web publication whose contributors conduct research using publically available materials such as information obtained from leakers and hackers. *See Id.* (Exh. F). Project PM’s work came to focus on the private military and intelligence contracting industry. This transition came amidst a federal crackdown on leaks escaping Washington and an attempt to prosecute whistleblowers.<sup>1</sup>

ProjectPM facilitated crowdsourcing<sup>2</sup> by design—it consisted of a webpage (wiki.echelon2.org), and an internet relay chat (IRC) channel (#ProjectPM). Project PM’s wiki

---

<sup>1</sup> For instance, Thomas Drake, a former agent with the NSA, had recently spoken openly about the government’s Trailblazer Project that was used to monitor private communication, and was charged under the Espionage Act for coming forth with that information. Josh Gerstein, Ex-NSA official takes plea deal. POLITICO, June 9, 2011. Original charges against him were dropped. *Id.*

<sup>2</sup> Crowdsourcing, put simply, is when a large group of people – usually in an online community – voluntarily contribute their time, ideas or material to a project.

hosted information that was based on traditional sources, in addition to information made publicly available by whistleblowers, leakers and hackers. The volume of information being acquired from non-traditional sources such as hacking and leaks was huge and ProjectPM leveraged the interest of concerned members of the public to help conduct transparency research. To this end, members of the public could contribute content to the ProjectPM webpage in conjunction with engaging in real-time discussions over IRC.

### **C. The Hack of Stratfor Forecasting, Inc.**

Strategic Forecasting, Inc., more commonly known as Stratfor, is a global intelligence company founded in 1996 in Austin, Texas, by George Friedman, who is the company's chairman. Stratfor has been cited by media as an authority on strategic and tactical intelligence issues. Barron's, the American weekly newspaper published by Dow Jones & Company since its founding in 1921, once referred to it as "The Shadow CIA."

According to a federal complaint in another case, "starting in December 2011" several alleged co-conspirators (not including include Mr. Brown) "obtained unauthorized access to Stratfor's computer systems." *United States v. Jeremy Hammond*, Sealed Complaint of March 12, 2012,<sup>3</sup> (hereinafter "Hammond Complaint") at 10. The FBI knew about (and, through their confidential informant, were orchestrating) the hack as early as December 6, 2011. *See Id.* at 13. At that time, Stratfor CEO George Freidman was notified that Stratfor's website was hacked and the "customer credit card and other information had been stolen." The next day, he "met with an

---

<sup>3</sup> *Available at:*

<http://www.justice.gov/usao/nys/pressreleases/March12/hackers/hammondjeremycomplaint.pdf> (last accessed March 2, 2014)

FBI special agent, who made clear that there was an ongoing investigation and asked for [Stratfor's] cooperation.”<sup>4</sup>

According to the Hammond Complaint, the Stratfor hack lasted until December 24, 2011, when news of the event became public. *Id.* However, according to the Hammond Complaint, unauthorized charges were made to credit card accounts as early as December 6, 2011. *Id.* at 13. For instance, on December 17, 2011 there was a donation given to Care.org from a stolen credit card.<sup>5</sup> According to the Hammond Complaint, data from the Stratfor hack was uploaded onto a server as early as December 19, 2011.

#### **D. Publication of Stratfor Files Occurred Before and After December 25, 2011**

According to the Hammond Complaint, the following was stolen from the system: “(1) approximately 60,000 credit card numbers and associated data, including Card Verification Values (CVVs) and expiration dates, belonging to Stratfor clients; (2) records for approximately 860,000 Stratfor clients or subscribers; (3) Stratfor employees’ emails; and (4) Internal Stratfor corporate documents, including company financial data.” *Id.* at 10.

On December 24, the Stratfor website was “defaced,”<sup>6</sup> notifying the world of the hack. According to Stratfor CEO George Freidman, “[t]he hackers published a triumphant note on [Stratfor's] homepage saying that credit card information had been stolen, that a large amount of email had been taken, and that four of our servers had been effectively destroyed along with data

---

<sup>4</sup> George Friedman, *The Hack on Stratfor*, Stratfor (Jan. 11, 2012 8:00), *available at* <http://www.stratfor.com/weekly/hack-stratfor> (last accessed March 2, 2014)

<sup>5</sup> See <http://www.f-secure.com/weblog/archives/stratfor1.png>

<sup>6</sup> Website defacement is an attack on a website that changes the visual appearance of the site or a webpage.

and backups.”<sup>7</sup> According to the Hammond complaint, “the Stratfor hack was first publicized in the media on December 24, 2011.” At 22. The reaction in the press was immediate and broad reaching. Hammond Sentencing Memo at 9.

On December 25, a document titled “Antisec teaser 12/25” was posted on a file sharing website. Hammond Complaint at 11. The document referenced stolen emails and financial information. *Id.* The document included several links to “what appeared to be files of stolen Stratfor data.” *Id.* On the same day, a document titled “Anonymous Lulzxcmas rooting your proud” was posted on a file sharing website. *Id.* The document, “included text that appears to demonstrate unauthorized access to Stratfor’s computer systems.” *Id.* The document referenced stolen emails and financial information. The document also included “what appears to be a link to a file of stolen Stratfor data.” *Id.*

On December 29, 2011, “online account information relating to approximately 860,000 Stratfor subscribers” was posted to an online location, as well as “approximately 60,000 credit cards numbers belonging to Stratfor clients.” *Id.* That day, a document titled “antisec teaser 12/26” was posted to a file sharing website. *Id.* at 11. The document referenced stolen emails and financial information. *Id.* The document included “what appear to be several links to stolen Stratfor data.” Three days later, on December 29, 2011, a document titled “antisec teaser 12/29 (legit)” was posted to a file sharing website. *Id.* The document referenced stolen emails and financial information. *Id.* The document included “what appear to be several links to stolen Stratfor data.” *Id.*

---

<sup>7</sup> George Friedman, *The Hack on Stratfor*, Stratfor (Jan. 11, 2012 8:00), <http://www.stratfor.com/weekly/hack-stratfor>. See also <http://arstechnica.com/tech-policy/2012/03/inside-the-hacking-of-stratfor-the-fbis-case-against-antisec-member-anarchaos/>.

The web pages referenced above are all still available online, as are the links they contain.<sup>8</sup> In addition, news agencies across the world reported these events, either republishing the above communiqués or linking to them from within articles. *See e.g.*, Olivia Katrandjian, *Hacking Group 'Anonymous' Takes First Step in 'Master Plan,' Vows to Strike Again*, ABC NEWS (Dec. 26, 2011),<sup>9</sup> Chloe Albanesius, *Hackers Dump More Stratfor Emails, Passwords*, PCMAG (Dec. 30, 2011),<sup>10</sup> *That Specializes in Security*, MASHABLE (Dec. 25, 2011).<sup>11</sup>

The incident touched on popular issues such as cybersecurity, government, and the private intelligence contracting industry. Cybersecurity experts across the world sifted through the stolen Stratfor data to conduct a forensic analysis of the hack. One video produced by CBS shows a forensics expert pointing at a screen containing stolen Stratfor data and talking about stolen credit card numbers.<sup>12</sup> Another cybersecurity expert, Richard Stiennon said, “the repercussions from the Stratfor emails could be as far reaching as the WikiLeaks release of 250,000 State Department cables.”<sup>13</sup> Many blamed Stratfor for failing to encrypt passwords.<sup>14</sup> Others saw great value in the emails being made public.<sup>15</sup>

---

<sup>8</sup> *See, e.g.* <http://pastebin.com/f7jYf5Wd>

<sup>9</sup> Available at: <http://abcnews.go.com/US/hacking-group-anonymous-vows-hit/story?id=15234349#.TvjoezUS01I>

<sup>10</sup> Available at: <http://www.pcmag.com/article2/0,2817,2398206,00.asp>, Zoe Fox, *Anonymous Hacks Company*

<sup>11</sup> Available at: <http://mashable.com/2011/12/25/anonymous-hacks/>

<sup>12</sup> *See* Anna Werner, Credit Cards hacked by Anonymous used in charity donations, CBS News, December 28, 2011 (available at:

<https://www.youtube.com/watch?v=bFCTMqGqKJs&noredirect=1>)

<sup>13</sup> *See*, Hackers Set to Dump Intel Analysis Firm’s Emails, WASHINGTON TIMES, Dec. 29, 2011 (available at [http://www.washingtontimes.com/news/2011/dec/29/hackers-set-to-dump-intel-analysis-firms-emails/?utm\\_source=RSS\\_Feed&utm\\_medium=RSS#ixzz2uvIWdCns](http://www.washingtontimes.com/news/2011/dec/29/hackers-set-to-dump-intel-analysis-firms-emails/?utm_source=RSS_Feed&utm_medium=RSS#ixzz2uvIWdCns))

<sup>14</sup> For instance, CNN’s Zoe Fox called the event “an embarrassing mistake for a company specializing in security.” Zoe Fox, *Anonymous Hackers Hit Security Group*, CNN, December 26, 2011 (available at <http://edition.cnn.com/2011/12/26/tech/web/anonymous-hack-stratfor/>)

<sup>15</sup> *See, e.g.*, Stratfor Emails reveal Secret, Widespread TrapWire Surveillance System, RT, (available at <http://rt.com/usa/stratfor-trapwire-abraxas-wikileaks-313/>); For instance, Journalist

### E. Conduct giving rise to the Indictment.

As discussed, *supra*, on December 25, 2011, document titled “Anonymous LulzXmas rooting your proud” was posted on a publicly available file sharing website. *See supra*, at 5. That document contained the following link:<sup>16</sup>

**[http://wikisend.com/download/597646/stratfor\\_full\\_b.txt.gz](http://wikisend.com/download/597646/stratfor_full_b.txt.gz)**

*See* Communiqué of December 25, 2011 (available at <http://pastebin.com/bUqkb9mq>)

Later that day at approximately 7:45PM, an IRC user published *the same link* on the #AnonOps IRC channel. Just moments after it appeared on the #AnonOps IRC channel, Mr. Brown republished the link on the #ProjectPM IRC channel. The link described the address of a website on a public server.<sup>17</sup> That website contained a file called `stratfor_full_b.txt.gz` (hereinafter “Stratfor file”).<sup>18</sup>

---

Amy Goodman, writing in The Guardian, referred to the first published leaks of Stratfor material as peering into an “intelligence-industrial complex.” Goodman, Amy, “Stratfor, WikiLeaks and the Obama administration’s War on Truth” THE GUARDIAN

<sup>16</sup> A link is an address of a website made up of a text string.

<sup>17</sup> Wikisend is a public website that is not restricted. Users navigating to a page on wikisend, such as that described here, are prompted to press a button before downloading any files contained therein.

<sup>18</sup> The Stratfor file is in compressed gzip format, as denoted by the .gz extension. As such, anyone wishing to see its contents would have to extract the plaintext file using a special archiving software or program.

## **ARGUMENT**

### **POINT I**

#### **THE COURT SHOULD DISMISS COUNT 1 & COUNTS 3–12 FOR FAILURE TO ALLEGE AN OFFENSE**

##### **A. The Legal Standard For Dismissal.**

Rule 12(b), F.R.Cr.P., provides in relevant part that “[a]ny defense, objection, or request that the court can determine without a trial of the general issue” may be raised before trial by motion. Rule 12(b)(3)(B) provides “at any time while the case is pending, the court may hear a claim that the indictment ... fails ... to state an offense.” *United States v. Payne*, 341 F.3d 393, 402 (5th Cir. 2003).

Courts have routinely held that for purposes of Rule 12(b)(3), “a charging document fails to state an offense if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation.” *United States v. Stock*, 728 F.3d 287, 291 (3d Cir. 2013); *United States v. Fontenot*, 665 F.3d 640, 644 (5th Cir. 2011) (“If a question of law is involved, then consideration of the motion is generally proper.” (quoting *United States v. Flores*, 404 F.3d 320, 324 (5th Cir. 2005))). Thus, a charge must be dismissed if the facts alleged in the charging document do not establish the crime charged. Here, Count 1 and 3–12 do not satisfy these constitutional and statutory standards.

##### **B. The Charging Statutes.**

###### **i. *Count 1 Charges a Violation of 18 U.S.C. §1028(a)(2)***

18 U.S.C. § 1028(a)(2) provides:

Whoever, in a circumstance described in subsection (c) of this section

[..]

(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority

[..]

shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 1028(a)(2).

18 U.S.C. § 1028(c)(3)(A) provides:

The circumstance referred to in subsection (a) is that

(3)(A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means;

18 U.S.C. § 1028(c)(3)(A).

**ii. *Counts 3–12 Charge Violations of 18 U.S.C. §1028A(a)(1)***

18 U.S.C. §1028A(a)(1):

Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

18 U.S.C.A. § 1028A.

According to subsection §1028A(c), all violations of §1028, with the exception of §1028(a)(7), qualify as predicates for §1028A(a)(1).<sup>19</sup>

**iii. *Count 1 is a Predicate of Counts 3–12.***

Counts 3–12 charge Mr. Brown with aggravated identity theft relating to his alleged violation of § 1028(a)(2). Accordingly, if Count 1 is dismissed, Counts 3–12 must fall as well.

---

<sup>19</sup> See §1028A(c)(4) (“any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028(a)(7)”).



### C. The Statutory Terms at Issue.

The terms at issue in this case are “transfer” and “authentication feature.” When the meaning of specific statutory language is at issue, courts first need to consider the meaning of particular words or phrases. *See In re Camp*, 631 F.3d 757, 759 (5th Cir. 2011) (“[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.” (quoting *Lamie v. U.S. Trustee*, 540 U.S. 526, 534 (2004))). To the extent any ambiguity exists, statutes imposing criminal liability must be construed strictly. This simply requires “that words [be] given their ordinary meaning and that any reasonable doubt about the meaning [be] decided in favor of anyone subjected to a criminal statute.” 3 Norman J. Singer, *Sutherland Statutes and Statutory Construction* § 59:3 (6th ed. 2005). This rule of strict construction is “buttressed by constitutional underpinnings” because convictions obtained by virtue of unforeseen judicial construction of criminal statutes violate the due process requirement that persons be provided with fair warning of criminalized conduct. *Duke v. Univ. of Texas at El Paso*, 663 F.2d 522, 527 (5th Cir. 1981).<sup>20</sup>

#### i. The meaning of “authentication feature” under § 1028.

The term “authentication feature” is defined by § 1028(d)(1) to mean:

any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the **issuing authority** on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;

*See* 18 U.S.C. 1028(d)(1) (emphasis added).

---

<sup>20</sup> *See also, Dunn v. United States*, 442 U.S. 100, 112 (1979); *Marks v. United States*, 430 U.S. 188, 191 (1977); *Rabe v. Washington*, 405 U.S. 313, 315 (1972); *Bowie v. City of Columbia*, 378 U.S. 347, 355 (1964).

In turn, the term “issuing authority” is defined by §1028(d)(6) to mean “any ***governmental entity or agency*** that is authorized to issue identification documents, means of identification, or authentication features,” §1028(d)(6)(A). As such, the definition of “authentication feature” means (1) holograms, symbols, codes, etc...; (2) used by ***a governmental entity or agency***; (3) on a document ***issued by that governmental entity or agency***; (4) to determine if the document is counterfeit, altered or otherwise falsified.

The source of the statutory definition is the SAFE ID Act of 2003.<sup>21</sup> The conference report for that legislation explains its purpose:

Under current law, it is not illegal to possess, traffic in, or use false or misleading ***authentication features whose purpose is to create fraudulent IDs***. [This section] would correct this oversight by making it a crime to counterfeit or alter “authentication features,” as well as to traffic such features in false identification documents or without the authorization of the appropriate authority. Authentication features are the holograms, symbols, codes, etc., ***used by the issuing authority to verify that an ID is authentic***. In addition, this section requires forfeiture of equipment used in creating or trafficking in illicit authentication features. This section will help the fight against child abduction, terrorism, identity theft, and underage drinking, among other things, by addressing the growing trade in illicit authentication feature for IDs.

H. Conf. Rep. No. 108–66, at 67 (2003), [2003 U.S.C.C.A.N. 683, 702] (emphasis added).

## ii. The meaning of “transfer” under § 1028.

The term “transfer” is partially defined in by §1028(d)(10) to *include*:

selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others; . . .

18 U.S.C. § 1028(d)(10) (emphasis added).

---

<sup>21</sup> Pub. L. No. 108–21, § 607, 117 Stat. 650, 689–91 (2003).

Where a word or phrase is defined in the statute, then that definition governs if applicable in the context used. Thus, at least as applied to the three delineated items,<sup>22</sup> §1028(d)(10) contemplates a method of transfer wherein the item is (1) selected and (2) placed on an online location (3) such that it is available to others. Otherwise, the plain meaning of the word governs.

Likewise, the plain meaning of “transfer” means “to convey from one person, place, or situation to another.” *Transfer Definition*, MERRIAM-WEBSTER DICTIONARY.<sup>23</sup> Defined as a legal term of art, transfer means “[t]o convey or remove from one place or one person to another; to pass or hand over from one to another, esp. to change over the possession or control of and [t]o sell or give.” BLACK’S LAW DICTIONARY (9th ed. 2009). While there is no Fifth Circuit case law that discusses the definition of the term “transfer” under §§1028 or 1028A, other Circuits have applied the Black’s Law Dictionary definition of the word transfer. *See e.g.*, *United States v. Hall*, 704 F.3d 1317, 1318 (11th Cir. 2013); *U.S. v. Spears*, 697 F.3d 592, 598 (7th Cir. 2012) (same).

#### **D. Count 1 Fails to Allege “Authentication Features” Within the Meaning of §1028.**

As discussed *supra*, Point I.C.ii., the statutory language of §1028 requires that an “authentication feature” be (or appear to be) issued by a “government entity or agency.”

---

<sup>22</sup> Section 1028(d)(3) defines “Identification Document” as “a document made or issued by or under the authority of the United States Government, a State political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance, a foreign government, political subdivision of a foreign government, an international government or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals.”

Section 1028(d)(2) defines “Document-making implement” as “any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement.”

<sup>23</sup> *available at*: <http://www.merriam-webster.com/dictionary/transfer>.

However, the “authentication features” alleged in the Indictment are Card Verification Values (“CVVs”). Indictment, 1–2. CVVs fail to satisfy the definition of “authentication feature” under §1028(d)(1) because they are issued by credit card companies, not a government entity or agency.<sup>24</sup>

While the Fifth Circuit has not construed the term “authentication feature,” the Fourth Circuit has held that prosecution under §1028 is limited to “authentication features” that are issued (or appear to be issued) by a governmental entity. *See United States v. Cline*, 286 Fed. Appx. 817, 820 (4th Cir. 2008). In *Cline*, the defendant was charged with violating §1028(a)(8) for trafficking in false authentication features. *Id.*, at 818. Section 1028(a)(8) is an analogous provision dealing with *false* authentication features. The *Cline* court interpreted the meaning of “authentication feature” under the statute:

Under § 1028(d)(1), an “authentication feature” is defined as a feature used by the “issuing authority” to determine whether the document is counterfeit. Pursuant to § 1028(d)(6), an “issuing authority” is ***limited specifically to governmental entities***.

*Id.*, at 820 n.2 (4th Cir. 2008) (emphasis added).<sup>25</sup>

---

<sup>24</sup> CVVs are issued to allow merchants to verify that a person using the card number has the card physically *in-hand* at the time of purchase. *See* 3-Digit Security Code, Visa available at [http://usa.visa.com/personal/security/visa\\_security\\_program/3\\_digit\\_security\\_code.html](http://usa.visa.com/personal/security/visa_security_program/3_digit_security_code.html); Financial Glossary and Terms, Discover Card, available at [https://www.discover.com/credit-cards/help-center/glossary.html?gcmpgn=0809\\_ZZ\\_srch\\_gsan\\_txt\\_1&srchQ=cid&srchS=internet\\_cm\\_corp&srchC=internet\\_cm\\_fe&srchP=0](https://www.discover.com/credit-cards/help-center/glossary.html?gcmpgn=0809_ZZ_srch_gsan_txt_1&srchQ=cid&srchS=internet_cm_corp&srchC=internet_cm_fe&srchP=0)

<sup>25</sup> Further supporting the plain meaning construction that requires “authentication features” be (or appear to be) issued by a government entity or agency is the term’s placement between “identification document” and “false identification document” throughout the statute. *See* §§1028 (a)(1–4), (b)(1)(A–B), (b)(2)(A); *see also*, *U.S. v. Jaensch*, 665 F.3d 83, 90 (4th Cir. 2011) (identification documents must appear to be issued by or under the authority of the United States); *U.S. v. Fuller*, 531 F.3d 1020, 1025 (9th Cir. 2008) (Only “[a] document made or issued by or under the authority of the United States Government” can be considered an identification document).

Conversely, no court has construed “authentication feature” without this requirement. Nor has any court construed CVVs to be “authentication features” under §1028. Moreover, interpreting “authentication feature” in the in the context of the whole statute leads to the ineluctable requirement of issuance by a government entity or agency. *See United Sav. Ass’n of Tex. v. Timbers of Inwood Forest Associates Ltd.*, 484 U.S. 365, 371(1988) (“[a] provision that may seem ambiguous in isolation is often clarified by the remainder of the statutory scheme”).<sup>26</sup>

First, a construction of “authentication feature” that encompasses CVVs would render the term “issuing authority” in Section 1028(d)(1), and the related term “government entity or agency” in Section 1028(d)(6) superfluous, which should be avoided. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (refusing to adopt statutory construction that would render statutory language “insignificant.”).

Second, CVVs and other information that is not issued by a government entity is encompassed by another term in the statute. That term, “means of identification,” is defined as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual.” §1028(d)(7). *See also* Indictment, Counts 3–12 (charging Mr. Brown with multiple counts of 1028A for transferring a “means of identification consisting of [...] CVVs.” Second, the transfer of CVVs and similar information is proscribed by another provision of the statute, §1028(a)(7), which prohibits the transfer of “means of identification [...] with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or

---

<sup>26</sup> *See also* 2 A J. Sutherland, *Statutes and Statutory Construction* § 47.02, at 139 (5th ed., Norman Singer ed.) (The Whole Act Rule instructs that subsections of a statute must be interpreted in the context of the whole enactment); *Kokoszka v. Belford*, 417 U.S. 642, 650 (1974) (“interpreting a statute, the court will not look merely to a particular clause in which general words may be used, but will take in connection with it the whole statute....”) (internal quotations omitted).

local law.” Unlike an “authentication feature,” the term does not require issuance by a “government entity or agency.”<sup>27</sup>

For these reasons alone, Count 1 and Counts 3–12 must be dismissed.

**E. Count 1 Fails to Allege a “Transfer” of CVVs.**

Even if the Court construes the term “authentication feature” to encompass CVVs, the indictment would still fail because the object of the “transfer” alleged in the Indictment is a hyperlink, not a file containing CVVs.

**i. *Hyperlink Mr. Brown is Alleged to Have Republished Did Not Contain CVVs***

The CVVs alleged in the Indictment were located in the Stratfor file. *See* Indictment at 1, 2, 4. As discussed *supra*, STMT FACTS, the Stratfor file was uploaded to public servers *by others* well before the commencement of the charged conduct. *Id.* Moreover, at no point does the Indictment allege the movement, conveyance or copying of the Stratfor file as part of the charged conduct. Nor does it allege Mr. Brown’s republication of an already public hyperlink caused the movement, conveyance or copying of the Stratfor file *at any time*.

Instead, the Indictment alleges the transfer of a hyperlink. A hyperlink is a path or address to a website, made up of a text string.<sup>28</sup> A hyperlink does not itself contain the content it

---

<sup>27</sup> This construction is in line with the purpose of the statute, the prevention of fraudulent identification documents. Read this way, the statute prohibits the knowing transfer of identity card making materials (such as “authentication features” found on a driver’s license) under 1028(a)(2), but, under 1028(a)(7) requires additional scienter for the transfer of items (such as CVVs) that cannot be used directly in the fabrication of false IDs.

<sup>28</sup> *See, e.g. Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 455 (2d Cir. 2001) (“The hyperlink can appear on a screen (window) as text, such as the Internet address (“URL”) of the web page being called up or a word or phrase that identifies the web page to be called up.”) cited in *U.S. v. Navrestad*, 66 M.J. 262 (C.A.A.F. 2008). *See also Perfect 10 v. Google, Inc.*, 416 F. Supp. 2d 828 (C.D. Cal. 2006), *aff’d* in part, *rev’d* in part and remanded on other grounds, 487 F.3d 701 (9th Cir. 2007), opinion amended and superseded on *reh’g*, 508 F.3d 1146 (9th Cir. 2007) and *aff’d* in part, *rev’d* in part and remanded, 508 F.3d 1146 (9th Cir. 2007) (“‘Link’ is

points to.<sup>29</sup> Thus, unlike sending an email attachment or uploading data to a website, republishing a hyperlink does not itself move, convey, select, place or otherwise transfer, a file or document from one location to another. *See ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1085 (Fed. Cir. 2003) (“The information sent. . . is not the information content itself, but rather a short text string—a URL—that identifies and locates content on the internet.”); *U.S. v. Navrestad*, 66 M.J. 262 (C.A.A.F. 2008)(same).

Thus, even if the Court were to construe the term “transfer” to include “selecting an [authentication feature] and placing it on an online location where it is available to others,” per §1028(d)(10), the indictment would still fail. Mr. Brown’s act in republishing a hyperlink did not result in the “selection” or “placement” of the Stratfor file containing CVVs. Rather, the government alleges only that Mr. Brown provided directions to where the Stratfor file was *placed by another person*. Because the republication of a hyperlink did not transfer the CVVs or any illicit content at all, Count 1 (and Counts 3-12) must be dismissed.

**ii. *By Republishing a Hyperlink, Mr. Brown Did Not Make the Stratfor File “Available To Other Persons Online”***

Rather than allege that Mr. Brown transferred the Stratfor file, the government alleges that “by transferring and posting the hyperlink, [Mr.] Brown caused the [Stratfor file] to be made available to other persons online.” Indictment at 2. However, at the time he allegedly republished the hyperlink, the Stratfor file was already public. The hyperlink also was already public. To uphold the indictment, therefore, would require the Court to construe the statute in a manner contrary to its plain language and congressional intent. *See* POINTS. I.B-C, *supra*.

---

most commonly used to refer to text or image ‘hyperlinks’ that are displayed on a webpage and that when clicked by the user, transport him to a new page.”).

<sup>29</sup> A hyperlink is “highlighted text or images that, when selected by the user, permit him to view another, related Web document.” *Bensusan Restaurant Corp. v. King*, 126 F.3d 25, 27 (2nd Cir. 1997).

First, republishing the hyperlink did not make the Stratfor file available to others. As explained above, the “hyperlink” was a text string that conveyed a location where the Stratfor file could be found, and nothing more. Second, the conveyance of information regarding the location of an unrestricted public website is not a crime under §1028(a)(2). To hold otherwise would stretch the statute far beyond the reach that Congress intended. *See* POINTS I.B-C, *supra*.

Third, even if the Court were to construe the term “transfer” to encompass “causing [data] to be made available to other persons online,” the indictment still fails because the Stratfor file (and its location) was already “available to [all] others” by virtue of their being in the public domain at the time of the charged conduct. *See*, STMT FACTS, *supra*. In addition, other persons had already published and pasted the hyperlink that Mr. Brown later allegedly copied and pasted. *Id.* The Stratfor file was a readily available publication, indexed and accessible by anyone in the public. Its location was pointed to (albeit indirectly) by media outlets across the globe.

As the Supreme Court discussed in *Reno v. American Civil Liberties Union*:

Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

*Reno v. American Civil Liberties Union*, 5121 U.S. 844, 852–3 (1997). By this analogy, Mr. Brown republished a card catalogue number to a book at the public library. Moreover, it was a card catalogue number everyone *already had access to*.

Fourth, the allegation that Mr. Brown “caused” authentication features “to be made available to other persons online” does not allege a sufficient *actus reus* to fit §1028(a)(2). Count 1 is a substantive charge and must allege a *completed* transfer of an “authentication feature.” *See* offense definition, BLACK'S LAW DICTIONARY (9th ed. 2009), (“A crime that is *complete* in itself



and is not dependent on another crime for one of its elements.”)(emphasis added)<sup>30</sup> Here, the government fails to allege that any person completed a “transfer” of authentication features, let alone Mr. Brown. As such, Count 1 (and Counts 3–12) must be dismissed.

**F. A dismissal of Count 1 (and Counts 3–12) would be in line with this Court’s ruling in *Live Nation Motor Sports, Inc.***

In *Live Nation*, this Court held that a webpage containing an embedded link enabling the web-surfer to listen to copyrighted audio on the webpage could qualify as a “public display or performance” in violation of the Copyright Act. *Live Nation Motor Sports, Inc. v. Davis*, 2006 WL 3616983 \*4 (N.D.Tx. 2006) (Lindsay).<sup>31</sup> The Court relied on *National Football League v. PrimeTime 24 Joint Venture*, a Second Circuit case that has held that “interpretation of the Copyright Act is to hold that a public performance or display includes each step in the process by which a protected work wends its way to its audience.” *Id.* (citing to *National Football League*).

First, *Live Nation* is a copyright case, and any holding therein should be limited to interpretation of the Copyright Act. Moreover, the rules of statutory construction did not require the strict construction mandated in criminal cases.

Second, the conduct complained of in *Live Nation* is materially distinguishable. In *LiveNation* the conduct is known as “inline linking”—where an infringing website acts as a portal or frame for infringed content sourced at another website. The “inline linking” on the

---

<sup>30</sup> Cf. Model Penal Code §5.01(b) (Official Draft, 1985) (if a particular result is an element of the crime, a person is guilty of attempt when they do or omit to do anything with the purpose if causing that result).

<sup>31</sup> The plaintiff in the case was SFX, a company that organized sport-motorcycling and “Supercross” events. SFX broadcast live coverage of these events over the internet free of charge, though the Web casts were accompanied by a number of sponsoring advertisements. The defendant was owner and operator of a super cross enthusiast site, and routinely linked directly to these webcasts, completely bypassing the ads and other content presented on the SFX website. The court granted a preliminary injunction against Davis, noting that his direct linking harmed SFX financially, and that SFX would likely prevail in its claims of copyright infringement.

infringer's site allowed the web-surfer to "display" (or listen to) protected material without having to leave the infringer's webpage. Courts have distinguished "in-line" linking in Copyright cases for purposes of liability. By contrast, "traditional" linking (as is alleged in this case) *transports* the user to the linked-to page without incorporating third-party content via "in-line" linking or framing. This has been held to not constitute direct infringement, in the copyright context,<sup>32</sup> even if the linked-to page is infringing.<sup>33</sup> The alleged republication of a hyperlink *in a chat room* cannot be described as "in-line" or "embedded" linking. Rather, utilization of a link requires opening a new web portal. This is more akin to a webpage that contains the link "www.NFL.com" in some non-embedded fashion. When the link is utilized, the user is transferred to a new window that displays the NFL's homepage.<sup>34</sup>

Finally, the rationale utilized in *LiveNation*—that "a public performance or display includes each step in the process by which a protected work wends its way to its audience"—is not applicable in this case. In *LiveNation* the illicit act of "public display or performance" is inexplicably intertwined with the harm intended to be mitigated by the act – misuse of

---

<sup>32</sup> See *Ticketmaster Corp. v. Tickets.Com, Inc.*, 54 U.S.P.Q.2d 1344 (C.D. Cal. 2000) (unpublished) ("[H]yperlinking does not itself involve a [direct] violation of the Copyright Act (whatever it may do for other claims) since no copying is involved."); *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004) ("[H]yperlinking per se does not constitute direct copyright infringement because there is no copying, [although] in some instances there may be a tenable claim of contributory infringement or vicarious liability."); *Bernstein v. JC Penney, Inc.*, 26 Media L. Rep. (BNA) 2471, 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998) (unpublished) (granting, without discussion, defendant's motion to dismiss on the ground that hyperlinking cannot constitute direct infringement); *Arista Records, Inc. v. Mp3Board, Inc.*, 2002 Copr. L. Dec. P 28483 (S.D. N.Y. 2002) (linking to content does not implicate distribution right and thus, does not give rise to liability for direct copyright infringement).

<sup>33</sup> *Arista Records, Inc. v. Mp3Board, Inc.*, 2002 Copr. L. Dec. P 28483 (S.D. N.Y. 2002).

<sup>34</sup> Surely had defendant in *Live Nation* placed a link on the "infringing" page that took web surfers to the SFX website, there would have been no lawsuit. In fact, companies often pay other websites to advertise in this way. See e.g. Google Ads

intellectual property.<sup>35</sup> Here, the mere act of republishing a hyperlink is not as intertwined with the harm.<sup>36</sup> Nor does the government here allege a completed transfer of authentication features. *Compare Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 137 (2d Cir. 2008) (Second Circuit observed that the transmission in *NFL* could only be considered a transmission “to the public” where it is but one link in a chain whose “final link was undisputedly a public performance.”) Indeed, it is unclear whether Mr. Brown’s alleged conduct resulted in *any harm*. Nor is the alleged “harm” (if any) contemporaneous. *See United States v. Am. Soc. of Composers, Authors, Publishers*, 627 F.3d 64, 74 (2d Cir. 2010)(“controlling significance [in the *National Football League* decision was due] to the fact that the immediately sequential downlink from the satellite to Canadian PrimeTime subscribers was a public performance of the games”)(citing *NFL* at 11–13).

Accordingly, Count 1 (and Counts 3-12) must be dismissed.

#### **G. Constitutional Avoidance Warrants Dismissal of Count 1 (and Counts 3–12).**

As demonstrated *infra*, POINTS II & III, this case raises several constitutional questions of first impression. Thus, interpreting §1028(a)(2) not to apply to Mr. Brown’s conduct is also warranted by the constitutional avoidance canon. Cases invoking the canon make clear that courts have consistently “avoided passing upon a large part of all the constitutional questions pressed upon it for decision.” *Ashwander v. TVA*, 297 U.S. 288, 346 (1936) (Brandeis, J., concurring); *see also Elk Grove Unified Sch. Dist. No. 1 v. Newdow*, 542 U.S. 1, 11 (2004).

---

<sup>35</sup> *Live Nation Motor Sports, Inc. v. Davis*, CIVA 3, 2006 WL 3616983 (N.D. Tex. Dec. 12, 2006) (See 17 U.S.C. § 102; *see also Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841 at 847 (2d Cir.1997) (citing H.R.Rep. No. 94-1476 at 52 (1976), reprinted in 1976 U.S.C.C.A.N. 5659 at 5665) (noting Congress's reasons for amending the Copyright Act to include protections for live broadcasts)).

<sup>36</sup> *E.g.* The receiver of the transfer would still have to utilize the authentication features to make a fake ID.

Thus, when the Supreme Court has been confronted with two plausible interpretations, one of which would raise a constitutional question and one of which would not, it has unhesitatingly adopted the latter reading. *See, e.g., Hooper v. California*, 155 U.S. 648, 657 (1895); *Mossman v. Higginson*, 4 U.S.12, 14 (1800). Accordingly, Count 1 (and Counts 3-12) must be dismissed.

## POINT II

### **THE COURT SHOULD DISMISS COUNT 1 & COUNTS 3-12 FOR PENALIZING CONDUCT PROTECTED BY THE FIRST AMENDMENT**

To the extent the Indictment survives the above analysis, and the Court rules that §1028 encompasses the conduct as alleged, Count 1 (and Counts 3-12) must be dismissed as an unconstitutional abridgement of the First Amendment. First, the allegations in this case are encompassed by the Supreme Court's holding in *Bartnicki v. Vopper*, in that Mr. Brown's publication of truthful information (by republishing a hyperlink) obtained in a lawful manner cannot be punished absent a showing of a heightened state interest. Second, Mr. Brown was engaged in pure political speech in republishing the hyperlink. Because §1028 as applied imposes a complete prohibition on such speech, and does so based on the speech's content, Count 1 (and Counts 3-12) must be dismissed absent a showing of a compelling state interest and least restrictive means. Finally, as applied to Mr. Brown, §1028 also fails the *O'Brien* test for intermediate scrutiny because it is not at parity with any substantial government interest that would be achieved less effectively absent regulation.

#### **A. The Application of §1028(a)(2) to Mr. Brown's Speech Warrants Strict Scrutiny**

##### ***i. Mr. Brown's Republication of a Hyperlink is Protected Speech.***

The First Amendment states that "Congress shall make no law ... abridging the freedom of speech." U.S. CONST. amend. I. All methods of expressing ideas, including movies, art,

books, and expressive physical conduct, are safeguarded by the free speech clause. *See, e.g., Texas v. Johnson*, 491 U.S. 397, 420 (1989) (holding that burning the American flag is expressive conduct that implicates the First Amendment); *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495, 502 (1952) (holding that “expression by means of motion pictures” is of First Amendment concern). Accordingly, Courts have generally found web hyperlinks to constitute speech. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 456 (2d Cir. 2001) (Hyperlink is expressive; conveys information, namely the Internet address of the linked web page).<sup>37</sup>

A principal aim of the First Amendment is to “secure the ‘widest possible dissemination of information from diverse and antagonistic sources.’” *New York Times Co. v. Sullivan*, 376 U.S. 254, 266 (1964) (quoting *Associated Press v. United States*, 326 U.S. 1, 20 (1945)). The First Amendment recognizes not only the speaker's right to share information but the public interest in receiving information. *See Thornhill v. Alabama*, 310 U.S. 88, 101-02 (1940) (“Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period.”)<sup>38</sup> Freedom of speech includes protection for discussions of governmental affairs. *See Buckley v. Am. Constitutional Law Found., Inc.*, 525 U.S. 182, 207 (1999).

In addition, First Amendment protection extends to publishers of news and information, including the press. *Sheppard v. Maxwell*, 384 U.S. 333, 350 (1966) (“unqualified prohibitions laid down by the framers were intended to give to liberty of the press the broadest scope that could be countenanced in an orderly society”) (quoting *Bridges v. State of California*, 314 U.S.

---

<sup>37</sup> *See also Sutcliffe v. Epping*, 584 F.3d 314, 329 (1st Cir.2009) (A municipality’s refusal to add a hyperlink to a private group's website constituted government speech).

<sup>38</sup> *Virginia State Bd. of Pharm. v. Virginia Citizens Consumer Council*, 425 U.S. 748, 756-57 (1976) (collecting cases on public's right to receive information).

252, 265 (1941)). However, First Amendment protection is not contingent on whether the speaker is “a trained journalist, formally affiliated with traditional news entities, engaged in conflict-of-interest disclosure, went beyond just assembling others’ writings, or tried to get both sides of a story.” *Obsidian Fin. Grp., LLC v. Crystal Cox* 740 F.3d 1284, 1291 (9<sup>th</sup> Cir. Jan. 17, 2014) (applying First Amendment protection to blogs).

**ii. 1028(a)(2) Seeks to Punish Pure Speech that is Political in Nature on the Basis of its Content.**

The following features of Section §1028 as applied here are critical to the First Amendment analysis, and mandate strict scrutiny. First, Mr. Brown is alleged to have engaged in pure speech, not merely conduct with expressive elements. The act of republishing a hyperlink is *unquestionably* an act of pure communication and expression. Thus, applying Section 1028 to Mr. Brown’s republication of a hyperlink is a substantial burden on his right to free speech. Pure speech also warrants the highest protection, and laws burdening pure speech must face heightened scrutiny. Only a “need ... of the highest order” can justify “a regulation of pure speech.” *Bartnicki*, 532 U.S. at 532, 526. *See, also, Cohen v. California*, 403 U.S. 15, 18 (1971) (treating conviction for wearing jacket with offensive message as based on pure speech, and subjecting it to heightened scrutiny); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 495 (1975) (same for conviction based on “pure expression” under Georgia rape shield law). Although §1028 may target non-speech conduct or conduct with incidental speech restrictions in other applications, its application to Mr. Brown’s republishing of a hyperlink targets pure speech. Therefore, strict scrutiny is warranted.

Second, Mr. Brown’s speech (by republishing the hyperlink) addressed political issues—namely the uncovering of improprieties within the private intelligence contracting industry. As such, it is entitled to the First Amendment’s highest protection. “[L]awful political speech [is] at

the core of what the First Amendment is designed to protect.” *Virginia v. Black*, 538 U.S. 343, 365 (2003); *see RAV v. City of St. Paul*, 505 U.S. 377, 422 (1992) ( “Core political speech occupies the highest, most protected position” constitutionally accorded to speech.)(Stevens, J., concurring); *First National Bank v. Bellotti*, 435 U.S. 765, 776 (1978) (political speech “is at the heart of the First Amendment’s protections”). Because political speech warrants such heightened protection, when a law burdens political speech, courts must apply “exacting scrutiny” and “uphold the restriction only if it is narrowly tailored to serve an overriding state interest.” *McIntyre v. Ohio Elections Comm’n.*, 514 U.S. 334, 347 (1995) (citation omitted).

Third, Mr. Brown’s speech (by republishing the hyperlink) was part of his routine press activity: gathering, disseminating and publishing information about the Stratfor hack and, more generally, private intelligence contractors.<sup>39</sup> *See Branzburg v. Hayes*, 408 U.S. 665, 707 (1972) (“News must not be unnecessarily cut off at its source ... for without freedom to acquire information the right to publish would be impermissibly compromised.”) (Stewart, J., dissenting, joined by J. Brennan and J. Marshall). §1028 as applied imposes a complete criminal prohibition on such speech. Section 1028 as applied bans such speech, rather than regulating it with time, place or manner restrictions, and as such, greater scrutiny is warranted.

Finally, §1028 as applied restricts speech based on content, by prohibiting speech (republishing of a hyperlink) if the hyperlink points to a website that contains content relating to stolen CVV’s, even if the speaker (Mr. Brown) had no part in stealing or publishing the CVV’s, producing that website, or producing that hyperlink. Laws that impose criminal bans on the basis of content trigger strict scrutiny. “A statute is presumptively inconsistent with the First Amendment” if it discriminates against “speakers because of the content of their speech.” *Simon*

---

<sup>39</sup> In addition, Mr. Brown was writing a book about “Anonymous.”

& *Schuster, Inc. v. Members of the New York State Crime Victims Board*, 502 U.S. 105, 115 (1991); *see also United States v. Playboy Ent. Group, Inc.*, 529 U.S. 803, 813 (2000) (“Since [the law] is a content-based speech restriction, it can stand only if it satisfies strict scrutiny.”).

**iii. Mr. Brown’s Conduct is Not “Speech Integral to Criminal Conduct.”**

Here, Mr. Brown’s republication of a hyperlink is not an integral part of the violation of §1028.<sup>40</sup> To the contrary, the alleged republication of a hyperlink occurred *after* (1) the unauthorized access of Stratfor Forecasting, (2) the acquisition of files from the Stratfor servers, (3) the posting of those files on a public server, and (4) the generation of the hyperlink referenced in the indictment. *See Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 250-51 (2002) (“*Ferber’s* judgment about child pornography was based upon how it was made, not on what it communicated.”)(Refusing to extend rationale to a federal ban on “virtual child pornography.”) Thus, as in *Ashcroft*, “the causal link is contingent and indirect. The harm does not necessarily follow from the speech, but depends upon some unquantified potential for subsequent criminal acts.” *Id.* 1402. Indeed, the government does not allege *any* harm caused by Mr. Brown’s republication of a hyperlink.<sup>41</sup>

---

<sup>40</sup> The Supreme Court has constructed a handful of narrow, precisely defined categories of expression that are not protected by the First Amendment at all. Among the excluded categories is speech integral to criminal conduct, *see, e.g., Giboney v. Empire Storage & Ice, Co.*, 336 U.S. 490 (1949). Conduct is “speech integral to criminal conduct” when “used as an integral part of conduct in violation of a valid criminal statute.” *New York v. Ferber*, 458 U.S. 747, 761-762 (1982) (quoting *Giboney*, at 498). In *Ferber* the Court ruled that child pornography is not protected speech because the market for child pornography was “intrinsically related” to the underlying abuse, and was therefore “an integral part of the production of such materials, an activity illegal throughout the Nation.” *Id.*, at 759, 761.

<sup>41</sup> Nor does the *Ferber* Court’s “dry-up-the-market” rationale apply here. First, the market for identity theft does not consist of journalists and activists sifting through public information to publish criticisms of the private intelligence industry. Moreover, Preventing the disclosure of the illegally obtained information is not one of the “rare occasions in which a law suppressing one party’s speech may be justified by an interest in deterring criminal conduct by another.” *Bartnicki*, at 1762. As the Court explained, in “cases relying on such a rationale ... the speech at



**B. Section 1028(a)(2) Cannot Survive Strict Constitutional Scrutiny.**

The factors discussed *supra*, Point II.A.ii., individually and taken as a whole, trigger strict scrutiny. A restriction on speech will fail strict scrutiny unless the law is necessary to further a compelling government interest and is narrowly tailored to serve that interest. *Brown v. Entertainment Merchants Ass'n*, 131 S.Ct. 2729 (2011). Regulations that cannot survive strict scrutiny are facially unconstitutional under the First Amendment. *See, e.g., Brown*, 131 S.Ct. 2729; *R.A.V.*, 112 S.Ct. 2538.

Under a strict scrutiny analysis, it is the government's burden to present a "compelling state interest," for which application of §1028 is necessary.<sup>42</sup> However, the general purpose of the statute—prevention of identification theft or fraud—does not constitute a sufficiently compelling state interest to warrant punishment. In addition, all of the asserted interests can be vindicated more directly and effectively by legislating meaningful criminal penalties for the misconduct that the government seeks to deter—the unlawful acquisition of information and its use to create fraudulent identification documents.

The Supreme Court has held in numerous cases that equally or more important state interests did not justify the suppression of speech. In *Bartnicki*, the Court noted that the case "present[ed] a conflict between interests of the highest order--on the one hand, the interest in the full and free dissemination of information concerning public issues, and, on the other hand, the interest in individual privacy" fortified by the right of the plaintiffs to engage in "private

---

issue is considered of minimal value." *Id.* at 1762 n. 13 (citing *Osborne*, 110 S.Ct. 1691; *Ferber*, 102 S.Ct. 3348).

<sup>42</sup> *See* Stephen A. Siegel, The Origin of the Compelling State Interest Test and Strict Scrutiny, 48 Am. J. Legal Hist. 355, 359-60 (2006)

speech.” *Bartnicki*, 532 U.S. at 518;<sup>43</sup> *see also Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 488 (1975) (Court recognized “right of privacy” insufficient to justify application of a statutory prohibition on the publication of the identity of a rape victim); *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 104 (1979) (“[M]agnitude of State’s interest” in the administration of criminal justice to seek to preserve the anonymity of a juvenile offender “not sufficient to justify application of a criminal penalty” to truthful speech about a matter of public concern.); *The Florida Star v. B.J.F.*, 491 U.S. 524, 537 (1989) (“highly significant” three governmental interests—“the privacy of victims of sexual offenses; the physical safety of such victims, ...; and the goal of encouraging victims of such crimes to report these offenses”—not “satisfactory served by imposing liability.”)

Here, by contrast, the government interest in prevention of identity theft or fraud, has no basis in a constitutional right. Nor is the application of 1028 to Mr. Brown sufficiently tailored to pass constitutional muster. This is particularly the case because the Stratfor file Mr. Brown is alleged to have “made available to others online” was already publicly available and widely disseminated at the time of the alleged conduct. Thus, punishing *further* dissemination would not have advanced *any* purported government interests related to the file’s availability. *See Florida Star*, at 535; *Bartnicki v. Vopper*, 532 U.S. at 546 (2001) (J. dissent). Moreover the government could achieve the same ends without targeting the common everyday expressive practice of republishing hyperlinks. Indeed, the statute if construed narrowly, see *supra*, POINT I., prevents the fraudulent production of identification documents without trampling on protected speech.

---

<sup>43</sup> *See also Bartnicki*, 532 U.S. at 532 (Citing the Brief for the United States, the Court recognized that Title III's restrictions are intended to protect the interest of privacy of communication thereby “encouraging the uninhibited exchange of ideas and information among private parties.” *Id.*)

**C. Applying *Bartnicki v. Vopper* to Mr. Brown's Republication of a Hyperlink Commands a Dismissal of Count 1 and Counts 3–12.**

In *Bartnicki v. Vopper*, 532 U.S. 514 (2001), the Supreme Court resolved an issue that is perfectly analogous to the facts of this case. The Court asked:

“Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the government punish the ensuing publication of that information based on the defect in a chain?”

*Id.*, at 528.

The Court in *Bartnicki* invalidated the application of §2511(1)(c) prohibiting disclosure of wiretaps obtained in violation of wiretap statutes, but received lawfully by media publishers. *Id.*, at 526. The Court applied strict scrutiny to the Federal Wiretap Act despite finding them content-neutral. *Id.* at 525–27. The majority also affirmed the Third Circuit's finding that the wiretapping statutes were prohibitions of “pure speech,” similar to “the delivery of a handbill or pamphlet.” *Id.* 526–27. Ultimately, the Court held that “if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.” *Id.*, at 545 (2001) (citing *Daily Mail*, at 103).

Application of *Bartnicki* commands a dismissal. First, Mr. Brown's alleged acquisition of a publicly available hyperlink was lawful. That the Stratfor file was obtained unlawfully *by another person* and stored on a public server *by another person* should not allow the government to punish Mr. Brown's protected speech “based on a defect in the chain.” *Bartnicki*, at 515.

In addition, the Stratfor hack was a matter of public significance. Indeed, as discussed *supra*, STMT FACTS, the event has been the subject of numerous news articles, lawsuits and public discussion at all levels. Moreover, issues of cybersecurity and the private intelligence

contracting industry are also a matters of public significance that have been subject to a great amount of press and public debate. *See Id.* Finally, §1028 does not further a state interest of the highest order sufficient to counterbalance the substantial burden on speech seen here. As discussed *supra*, POINT II.B., and *infra*, POINT II.D., the application of §1028 to Mr. Brown’s speech (by republication of a hyperlink) does nothing to further a government interest of preventing the production of fraudulent identification documents.

As the Supreme Court has noted, “state action to punish the publication of truthful information seldom can satisfy constitutional standard,” *Daily Mail*, 443 U.S. at 102, because imposition of “a penal sanction for publishing lawfully obtained, truthful information ... requires the highest form of state interest to sustain its validity.” *Daily Mail*, 443 U.S. at 101-02. Thus, the First Amendment's protections may properly be divested, but “only in exceptional cases”<sup>44</sup> This is not one of them.

**D. Section 1028(a)(2) Cannot Survive Intermediate Constitutional Scrutiny.**

Should the Court determine that §1028 is properly treated as content-neutral, rejecting *Bartnicki*, the statute will be subject to the intermediate scrutiny test. Under *O'Brien*, a content-neutral regulation will be sustained if:

“it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.”

*United States v. O'Brien*, 391 U.S. 367, 88 S.Ct. 1673, 1698 (1968).

---

<sup>44</sup> To date, the Court has defined such “exceptional cases” narrowly to include the following circumstances: “[W]hen the country is at war, when a sovereign seeks to protect the primary requirements of decency by prohibiting obscenity, and when the security of community life is threatened by incitements to acts of violence and the overthrow by force of an orderly government.” *Worrell Newspapers of Indiana, Inc. v. Westhafer*, 739 F.2d 1219, 1223 (7th Cir. 1984) *aff’d sub nom. Westhafer v. Worrell Newspaper of Indiana, Inc.*, 469 U.S. 1200 (1985).

The principal interest asserted by the government—protecting victims of identity theft from the additional injury allegedly caused by dissemination of their information—is by no means insubstantial. However, both the hyperlink and the Stratfor File were *already public* before Mr. Brown’s alleged conduct. Thus, any application to Mr. Brown’s re-publication of a publicly available hyperlink, directing others to an already publicly available file, no longer “furthers an important or substantial government interest” in any meaningful sense. *See United States v. National Treasury Employees Union*, 513 U.S. 454, 475 (1995).

Indeed, the government has not alleged a single illicit credit-transaction and/or identity theft that was caused by Mr. Brown’s alleged republication of the hyperlink.<sup>45</sup> Thus, any “additional injury allegedly caused by the alleged republication of the hyperlink is [ ] related to the suppression of free expression.” *O’Brien*, 391 U.S. at 377. That fact, alone, renders Section 1028’s application constitutionally invalid. *See Buckley v. Valeo*, 424 U.S. 1, 17 (1976).

In addition, §1028 is not “narrowly tailored” to serve any of the asserted interests without restricting First Amendment freedoms to a greater degree “than is essential.” *O’Brien*, 391 U.S. at 377. As mentioned above, republication of a hyperlink has no meaningful effect on the asserted interests, and thus restricting such action is non-essential. In addition, all of the asserted interests can be vindicated more directly and effectively by legislating meaningful criminal penalties for the misconduct that the Government seeks to deter—the unlawful acquisition of information and its use to create fraudulent identification documents.

Most significantly, §1028 prohibits the dissemination of considerably more speech than is necessary. The statute prohibits *any* transfer of an authentication feature or identity document by

---

<sup>45</sup> Mr. Brown has asked the government for such information on numerous occasions. The government has indicated that it cannot show a connection between Mr. Brown’s republication of the hyperlink and a single transfer of authentication features, transfer of CVVs and/or illicit credit card transactions.

*anyone*, even in the absence of fraudulent intent. As applied, the government asks the Court to construe this to encompass republication of the *public location* of such items, a restriction on free expression that extends well beyond the transfer of an authentication feature or identity document to encompass critical public discussion and exchange of ideas. And as this case demonstrates, if §1028 is construed to apply here, that would allow prosecutors unfettered discretion in choosing among a wide variety speech-actors someone to prosecute, thereby exacerbating the First Amendment harms.

### POINT III.

#### **THE COURT SHOULD DISMISS COUNTS 1 AND COUNTS 3–12 AS UNCONSTITUTIONALLY VAGUE AND OVERBROAD**

As the foregoing analysis demonstrates, the conduct alleged against Mr. Brown is not encompassed by §1028 or §1028A. However, if, notwithstanding the plain meaning, the legislative history, somehow the alleged conduct is deemed within the charging statutes, §§ 1028 & 1028A would be unconstitutionally vague on their face and as applied. In addition, they would be unconstitutionally overbroad and chill speech in violation of the First Amendment.

##### **A. Sections 1028(a)(2) is Unconstitutionally Vague on its Face**

Vague laws offend two aspects of the Fifth Amendment's Due Process guarantee: they fail to provide adequate notice of what conduct is proscribed, and the lack of definable standards makes them susceptible to arbitrary and discriminatory enforcement. *Grayned v. City of Rockford*, 408 U.S. 104, 108-09 (1972). The degree of precision required increases with the gravity of the penalty and the importance of the rights at stake. *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982) (higher standard applicable for criminal statutes and when speech at stake). The facts of this case amply demonstrate the pernicious impact of both vices.

As discussed *supra*, **Point I.D.**, any construction of the statute that survives dismissal in this case would necessarily render the terms “issuing authority,” §1028(d)(1), and “government entity or agency,” §1028(d)(6), meaningless. As such, §1028 would be read as prohibiting, *inter alia*, “the knowing transfer of an authentication feature” with the term “authentication feature” defined as, *inter alia*, a “number [...] on a means of identification [...] used to determine if the document is counterfeit, altered, or otherwise falsified.” § 1028(d)(1). The same statute, however, prohibits the transfer or possession of a “means of identification” with fraudulent intent, §1028(a)(7) defining a “means of identification” as, *inter alia*, a number that may be used to identify a specific individual. §1028(d)(7). In addition, §1028A imposes an additional punishment for possession of a “means of identification” whilst violating §1028(a)(2), but not §1028(a)(7).

Thus, a person of ordinary intelligence would have no meaningful notice as to whether it was a crime to knowingly possess or transfer an item that satisfies all the requirements of an authentication feature but is not issued by a government entity. Likewise, as to 1028A, that same person would have no notice that harboring a *more culpable* mens rea (intent to defraud) might actually result in a charge of 1028(a)(7) for which the aggravated 1028A charge (carrying a mandatory two year sentencing increase) *cannot* be lodged. The prospect for discriminatory enforcement implicit in such imprecise construction is also likely.

#### **B. As Applied to Mr. Brown Section 1028(a)(2) is Unconstitutionally Vague**

The statute as applied to Mr. Brown is vague for a number of reasons. Mr. Brown is alleged to have violated §1028(a)(2)—which prohibits the “knowing transfer of an authentication feature without lawful authority”—for allegedly republishing a hyperlink that was already in the public sphere before the event. First, he cannot tell from the plain language if the meaning of

“transfer” includes republication of a (public) hyperlink, which contains only location information in a text string. Second, he cannot tell from the language that the statute proscribes re-publication of a hyperlink that already was publicly available, and that indicated a location to a file that already had been made publicly available. Third, he cannot tell from the statute that the meaning of “issuing authority,” “government entity” and “authentication feature” might apply to CVV’s that are issued by non-governmental entities.

The prospect for discriminatory enforcement implicit in such imprecise construction is likely. Mr. Brown is alleged to have violated §1028(a)(2)—which prohibits the “knowing transfer of an authentication feature without lawful authority”—for allegedly republishing a hyperlink that was already in the public sphere before the event. Mr. Brown’s conduct was clearly not intended to pursue counterfeiting activities as demonstrated both by his comments (on IRC Chat and to the public) and the fact that there is no alleged fraudulent purpose. Indeed, to date the government has yet to allege any harm that the alleged republication of a hyperlink has caused.

The uncertainty of the charges, and how they match up to the conduct as alleged has already caused a great deal of uncertainty among members of the public. For instance, such a construction of the statutory terms leaves one uncertain as to whether press activities such as newsgathering and research (e.g. by downloading content from a public website), or verification of sources (e.g. by reading that content), are fair or foul, a status inviting discriminatory enforcement of the statute. This is particularly the case for §1028(a)(2), which fails to require any malicious intent. This is especially vague to journalists who may have constructive knowledge of a fact, yet have a duty to inspect information to verify their sources.



This construction also significantly chills scientific research conducted by private cybersecurity researchers for the same reasons. Private security researchers are often depended on by companies like Stratfor to conduct unsolicited forensic analysis of data dumps in order to find out who conducted the hacks and how future attacks can be avoided. *See* Nicole Perlroth, Reporting from the Web's Underbelly, NY TIMES, Feb 16, 2014. In doing so, these security researchers (many of whom analyzed the Stratfor hack) knowingly transfer hacked data onto their systems. *See Id.*

Finally, even if the categorical speech prohibitions of §1028 are sufficiently precise to give fair warning of proscribed conduct, they are unconstitutionally overbroad in that they also suppress protected speech.

**C. § 1028(a)(2) is Overbroad Because it Prohibits a Substantial Amount of Protected Speech.**

According to the “First Amendment[’s] overbreadth doctrine, a statute is facially invalid if it prohibits a substantial amount of protected speech.”<sup>46</sup> Here, §1028(a)(2)’s overbreadth is implicit in its categorical approach toward prohibited speech. The statute prohibits a range of activities protected by the first amendment by banning the possession and transfer of certain items regardless of the circumstances surrounding the transfer. Nor does it distinguish information that has already “leaked” to the public (making the effect of prohibition moot). Nor does it require specific intent, inconsistent with decades of First Amendment jurisprudence.<sup>47</sup>

As such, the statutory prohibition does not distinguish between transfer for nefarious purposes (such as fraud) and that which is clearly protected First Amendment activity. The range of activities prohibited is wide, particularly given the public’s dependence on information

---

<sup>46</sup> *Hersh v. U.S. ex rel. Mukasey*, 553 F.3d 743, 762 (5th Cir. 2008).

<sup>47</sup> *See Scales v. United States*, 367 U.S. 203, 229-30 (1961)(First Amendment prohibits proscription of speech without requirement of specific intent).

that is the result of leaked information. As discussed above, the activities prohibited include those of everyday members of the public desiring to conduct research on the internet, cyber security researchers who wish to analyze and prevent cyber-attacks and journalists who wish to publish the news or perform critical (albeit routine) press activities such as newsgathering and source verification.

As such, persons of ordinary firmness would certainly experience chilling of their First Amendment rights. Accordingly, §1028(a)(2) is substantially, and fatally overbroad.

### **CONCLUSION**

For the above reasons, the Court should grant this motion in its entirety and dismiss Count 1 (and Counts 3–12).

Respectfully submitted,

-s- Ahmed Ghappour  
AHMED GHAPPOUR  
*Pro Hac Vice*  
Civil Rights Clinic  
University of Texas School of Law  
727 East Dean Keeton St.  
Austin, TX 78705  
415-598-8508  
512-232-0900 (facsimile)  
aghappour@law.utexas.edu

CHARLES SWIFT  
*Pro Hac Vice*  
Swift & McDonald, P.S.  
1809 Seventh Avenue, Suite 1108  
Seattle, WA 98101  
206-441-3377  
206-224-9908 (facsimile)  
cswift@prolegaldefense.com

MARLO P. CADEDDU  
TX State Bar No. 24028839  
Law Office of Marlo P. Cadeddu, P.C.

3232 McKinney Ave., Suite 700  
Dallas, TX 75204  
214.744.3000  
214.744.3015 (facsimile)  
mc@marlocadeddu.com

*Attorneys for Barrett Lancaster Brown*

CERTIFICATE OF SERVICE

I certify that today, March 5, 2014, I filed the instant motion using the Northern District of Texas's electronic filing system (ECF) which will send a notice of filing to all counsel of record.

/s/ Ahmed Ghappour

AHMED GHAPPOUR

/s/ Charles Swift

CHARLES SWIFT

/s/ Marlo P. Cadeddu

MARLO P. CADEDDU

*Attorneys for Barrett Lancaster Brown*